ORIGINAL

BEFORE THE

Federal Communications Commission

WASHINGTON, DC 20554

DOCKET FILE COPY ORIGINAL

In the Matter of	)	
	)	
Communications Assistance	)	CC Docket No. 97-213
for Law Enforcement Act	)	

AIRTOUCH COMMUNICATIONS, INC. REPLY COMMENTS

AIRTOUCH COMMUNICATIONS, INC.

Pamela J. Riley
David A. Gross
1818 N Street, N.W.
Suite 800
Washington, D.C. 20036
(202) 293-3800

Michael W. Mowery
AirTouch Communications, Inc.
2999 Oak Road, MS1025
Walnut Creek, CA 95596
(510) 210-3804

Attorneys for AirTouch Communications, Inc.

June 12, 1998

TABLE OF CONTENTS

Summary

The Commission should dismiss the rulemaking petition filed by the Department of Justice and Federal Bureau of Investigation ("DOJ/FBI") because they have failed to demonstrate that the industry standard is deficient or that any of their punch list items are required by the Communications Assistance for Law Enforcement Act ("CALEA"). In fact, even DOJ/FBI concede that some of the capabilities and solutions they desire are *not* required by CALEA.

CALEA authorizes the Commission to impose a new capability on industry only if it can be deployed "by cost-effective means." Although DOJ/FBI claim their punch list can be deployed by cost-effective means, they have failed to make available the vendor cost estimates in their possession. If DOJ/FBI fail to make this critical data available with their reply comments, one can only conclude that the data is not helpful to their position. Indeed, based on general cost estimates provided, it appears that implementation of the punch list items would be enormously expensive. The Commission should summarily reject the DOJ/FBI petition if they choose not to make this critical cost data available for the record and for public comment.

DOJ/FBI now concede that many of the capabilities they seek could be implemented in more than one way. CALEA makes clear, however, that *carriers* retain the right to decide how to implement the statute's requirements and that the government does not have the authority to direct carriers to implement one particular CALEA solution. Further, the DOJ/FBI argument that the Commission should dictate solutions constitutes an improper attempt to shift costs of non-mandated solutions from their own budgets to carriers.

The Commission should also reject the petition filed by the Center of Democracy and Technology ("CDT") challenging the industry standard. The first CDT issue, CMRS location, has been effectively rendered moot by virtue of the FBI's concession that law enforcement may receive limited location information only with a Title III, call content interception order. Nor is the industry standard deficient regarding the second CDT issue, involving packet data. The industry standard leaves it to the courts to determine the appropriate circumstances in which law enforcement may receive packet data — the resolution of which will almost certainly require a case-by-case approach based on the circumstances presented in each application for an interception order.

AirTouch believes the industry standard meets fully CALEA's assistance capability requirements. However, if the Commission disagrees, it should refer any additional standards work to the TIA standards subcommittee, TR-45.2. The DOJ/FBI opposition to referral to TR-45.2 lacks merit; indeed, referral would actually facilitate the very interests which DOJ/FBI have articulated.

It is agreed by all that the industry standard which the Commission is currently considering applies only to landline carriers, cellular carriers, and broadband PCS licensees — and does not apply to other telecommunications technologies such as paging. The Commission should confirm in its order in this proceeding that the scope of any new rules or requirements adopted will apply at most to landline carriers, cellular carriers, and broadband PCS licensees.

Finally, it is premature for the Commission to invoke its authority under Section 109 of CALEA, as a handful of commenters apparently request. Among other things, the Commission is currently examining the factors it should consider as part of a Section 109 analysis, and industry obviously cannot address these factors until the Commission completes this rulemaking.

BEFORE THE

Federal Communications Commission

WASHINGTON, DC 20554

In the Matter of	)	
	)	
Communications Assistance	)	CC Docket No. 97-213
for Law Enforcement Act	)	

AIRTOUCH COMMUNICATIONS, INC. REPLY COMMENTS

AirTouch Communications, Inc. ("AirTouch") submits this reply in response to the comments filed on May 20, 1998.[1] The comments persuasively — and overwhelmingly — demonstrate that the Commission must deny the Joint Petition for Expedited Rulemaking filed by the Department of Justice and the Federal Bureau of Investigation (collectively, "DOJ/FBI"). Indeed, even DOJ/FBI concede that some of the capabilities and solutions they desire are *not* required by the Communications Assistance for Law Enforcement Act ("CALEA").

The Commission should also reject the petition filed by the Center for Democracy and Technology ("CDT"), which contends the industry standard goes too far in two respects. The first CDT issue, CMRS location, has been effectively rendered moot by virtue of the FBI's concession that law enforcement may receive limited location information only with a Title III,

---

[1] Comments were filed by: AirTouch Communications (AirTouch"); Americans for Tax Reform, Center for Technology Policy, and Citizens for a Sound Economy ("ATR/CTP/CSE"); Ameritech Operating Companies ("Ameritech"); AT&T Corp. ("AT&T"); BellSouth Corp. ("BellSouth"); Cellular Telecommunications Industry Association ("CTIA"); Center for Democracy and Technology ("CDT"); Department of Justice and Federal Bureau of Investigation ("DOJ/FBI"); Electronic Privacy Information Center, Electronic Frontier Foundation, and American Civil Liberties Union ("EPIC/EFF/ACLU"); GTE Service Corp. ("GTE"); Nextel Communications ("Nextel"); New York City Police Department ("NYPD"); Personal Communications Industry Association ("PCIA"); PrimeCo Personal Communications ("PrimeCo"); SBC Communications ("SBC"); Sprint Spectrum ("Sprint"); Telecommunications Industry Association ("TIA"); United States Telephone Association ("USTA"); and U S WEST, Inc. ("U S WEST").

call content interception order. Nor is the industry standard deficient regarding the second CDT issue, involving packet data. The industry standard merely leaves it to the courts to determine the appropriate circumstances in which law enforcement may receive packet data — the resolution of which will almost certainly require a case-by-case approach based on the circumstances presented in each application for an interception order.

In the end, the DOJ/FBI and CDT petitions, though raising very different issues, share the same flaw: neither petition affirmatively demonstrates that industry improperly discharged the duty Congress delegated to industry. Congress specified the assistance capability requirements in general terms only, and it imposed on industry the "key role in interpreting the legislated requirements and finding ways to meet them without impeding the deployment of new services," subject, of course, to review by the Commission.[2] While CDT and DOJ/FBI contend that industry did not properly draw the line Congress asked industry to draw, the record demonstrates that the industry standard should be affirmed because it falls within both the floor and ceiling Congress has established.[3] Accordingly, the Commission should reject the DOJ/FBI and CDT petitions.

I. The Commission Should Dismiss the DOJ/FBI Petition for Rulemaking

Congress made clear that CALEA was designed to "preserve . . . not expand" law enforcement's surveillance capabilities, and it directed "industry, law enforcement and the FCC to narrowly interpret [CALEA's] requirements."[4] In this regard, the FBI Director assured Congress that CALEA would "preserve the status quo" and provide law enforcement with "no

---

2 H.R. Rep. No. 103-827 at 19 (1994)("House Report").

3 *See id.* at 22.

4 House Report at 9, 12, 13, 17, and 23.

more and no less information than it had in the past."[5] Now, however, DOJ/FBI admit they seek to use CALEA to obtain "new information . . . not previously received."[6] Given the governing statutory standard, the Commission must reject the DOJ/FBI petition for rulemaking.

A. The Commission Should Summarily Dismiss the DOJ/FBI Petition Unless They Submit Critical Cost Data

The comments note the importance of cost implementation data as part of the Commission's statutory review of the DOJ/FBI Petition.[7] Indeed, Congress has specified that the Commission may impose a controversial capability only if it "meets the assistance capability requirements of section 103 *by cost-effective methods.*"[8] Congress has further directed the Commission to adopt standards that "minimize the cost" of CALEA compliance on residential consumers.[9]

DOJ/FBI have contended in their petition that their "punch list" capabilities can be deployed "by cost-effective methods" and with minimal cost impact on residential consumers.[10] At the time DOJ/FBI made their claims, they did not have access to vendor cost estimates and their claims were, by definition, untested and speculative. However, DOJ/FBI *now*

---

5 *Id.* at 22.

6 DOJ/FBI Petition at 26 ¶ 45. There is, therefore, no basis to DOJ/FBI's conflicting representation that they "simply seek access to information that the carrier necessarily processes and maintains." *Id.* at 60 ¶ 109.

7 *See, e.g.,* AirTouch at 4-5; Nextel at 5; PrimeCo at 10 and 13; U S WEST at 22 and 26.

8 47 U.S.C. § 1006(b)(1)(emphasis added).

9 *Id.* at § 1006(b)(2).

10 *See* DOJ/FBI Petition at 59-62 ¶¶ 107-11.

have access to vendor cost estimates to develop the punch list items,[11] and while AirTouch has not been given access to the information supplied to the FBI, it is AirTouch's understanding that these cost estimates are huge. In this regard, one vendor has advised AirTouch that work involved in developing the punch list alone would exceed — by 160% — the substantial effort required to develop the modifications required by the industry standard.[12]

The Commission requires this cost data to apply the governing statutory criteria. Congress further specified that the Commission's process in applying the statutory criteria "must be made public."[13] Consequently, it is imperative that this financial data be made publicly available (without, of course, attributing specific cost estimates to particular vendors), and interested parties should be given the opportunity to comment on this data.

If DOJ/FBI fail to make this critical data available, one can only conclude that the data is not helpful to their position — that is, the punch list items cannot be deployed "by cost-effective methods."[14] Consequently, and given the statutory criteria which it must apply, the Commission should summarily reject the DOJ/FBI Petition if they choose not to make this critical cost data available for the record and for public comment.

B. The DOJ/FBI Proposed "Most Effective Means" Test Is Inconsistent With CALEA and Constitutes an Improper Attempt to Shift Costs to Consumers

Section 103 of CALEA specifies the interception capabilities carriers are to provide law enforcement. Congress was very clear that each carrier possessed considerable

---

11 *See, e.g.* U S WEST at 22 and 26.

12 *See* AirTouch at 9.

13 House Report at 27.

14 47 U.S.C. § 1006(b)(1).

flexibility in determining *how* to implement these capabilities within its network. Among other things, Congress expressly declared that law enforcement may neither require carriers to use any specific solution nor prohibit carriers from adopting solutions they prefer to use.[15] While Congress encouraged industry to adopt implementing standards, it further made clear that "[c]ompliance with the industry standards is voluntary, not compulsory. Carriers can adopt other solutions for complying with the capability requirements."[16]

DOJ/FBI now concede that many of the capabilities they seek "could be implemented in more than one way."[17] For example, DOJ/FBI readily acknowledge that carriers can provide surveillance status information "by a variety of means."[18] Nevertheless, they claim that the Commission "must" require "automated delivery" of this information because, in their view, "manual delivery . . . is simply no longer adequate."[19] According to DOJ/FBI, the Commission "must . . . add" any capability or solution which law enforcement determines constitutes "the most effective means" by which they can access the information.[20]

There are two fundamental flaws with DOJ/FBI proposed "most effective means" standard. First, DOJ/FBI are asking the Commission to legislate *solutions*, when Congress made very clear that solutions were to be determined *by each carrier*, and not by the government

---

15 *See* 47 U.S.C. § 1002(b)(1).

16 House Report at 27.

17 DOJ/FBI at 6 ¶ 7.

18 DOJ/FBI Petition at 53 ¶ 97.

19 DOJ/FBI at 12 ¶ 21, 13 ¶ 24, and 14 ¶ 25.

20 *Id.* at 6 ¶ 7 and 12 ¶ 21. *See also id.* at 14 ¶ 25, where the FBI instead characterizes its proposal as "the most appropriate way" test.

(whether law enforcement or the Commission). Second, assuming *arguendo* it was appropriate for the Commission to legislate solutions, the solutions adopted must reflect the "most effective means" *for carriers*, not law enforcement. This is clear from the Congressional directive that the Commission should "minimize the cost" of CALEA compliance on residential telecommunications users.[21] Indeed, it is apparent that many of the DOJ/FBI requests constitute nothing more than an improper attempt to shift costs of non-mandated solutions from their own budgets to carriers and their customers.[22]

C. There Is No Basis to Impose an Enhanced Conference Call Requirement on Carriers

DOJ/FBI correctly observe that CALEA's purpose is to ensure that changes in telecommunications technologies "do not frustrate law enforcement's continued ability to carry out legally authorized electronic surveillance."[23] Notwithstanding this acknowledged limited Congressional purpose, DOJ/FBI now want the Commission to use CALEA as a tool to *expand* the capabilities carriers provide to law enforcement. One example is the FBI's proposed enhanced conference call feature, whereby law enforcement wants the right to intercept, without

---

21 *See* 47 U.S.C. § 1006(b)(3).

22 Under CALEA, carriers are responsible for underwriting the costs of meeting the assistance capability requirements for equipment "installed or deployed" after January 1, 1995. 47 U.S.C. § 1008. If, however, the Commission rejects the DOJ/FBI punch list, law enforcement will, like any other customer, acquire solutions such as automated delivery of surveillance status only if they pay carriers their costs to implement the capabilities in question.

23 FBI at 3 ¶ 2. *See also* House Report at 9, 12, 13, 17, and 23.

obtaining an additional court order, the communications of persons not specified in the existing court order.[24]

DOJ/FBI respond that obtaining an additional court order is unnecessary because they may lawfully intercept the communications not only of persons identified in the court order but also other persons which use the intercept subject's telephone.[25] However, interceptions of these "other" communications are permitted because there is a nexus with the intercept subject (*i.e.,* use of the subject's telephone). In addition, as DOJ/FBI recognize, these "other" communications are subject to the statutory "minimization" requirement.[26] With their proposed enhanced conference call feature, there is no nexus between the interception subject identified in the court order and the communications sought to be intercepted. In addition, given the minimization requirement, there is no justification to intercept any of the desired communications because law enforcement would know *before* the interception occurs that the interception subject is no longer participating in the conference call and that the interception would be directed solely at non-targets. Importantly, Congress has cautioned the Commission "against overbroad interpretation of the [assistance capability] requirements":

> *The Committee expects* industry, law enforcement and *the FCC to narrowly interpret the [capability] requirements.*[27]

---

24 Although DOJ/FBI have readily admitted that this is an entirely new capability (*see* Joint Petition at 30 ¶ 51), they remarkably claim that their proposal is "fully consistent with the overriding purpose of CALEA . . . '*to preserve* the government's ability * * * to intercept communications.'" DOJ/FBI at 8 ¶ 12 (emphasis added).

25 *See* DOJ/FBI at 7-8 ¶ 11.

26 *Id.* at 8 ¶ 11.

27 House Report at 22-23 (emphasis added).

Finally, practical considerations militate against deployment of this controversial feature. As numerous commenters point out, criminals could easily bypass any enhanced conference call feature which carriers might deploy simply by using the conference bridge services of an independent provider.[28] In these circumstances, there is no basis for the Commission to require industry to deploy the proposed enhanced conference call feature.

D. Much of the Information DOJ/FBI Seek Is Not Call-Identifying Information Under CALEA

DOJ/FBI have asked the Commission to require carriers to provide "all dialing or signaling information."[29] This request far exceeds the scope of CALEA, which specifies that call-identifying information shall be limited to that "dialing or signaling information that identifies the *origin, direction, destination, or termination* of each communication."[30] The comments demonstrate that the following punch list items fall outside the scope of this statutory definition because they do not identify "the origin, direction, destination, or termination" of a communication:

- Punch list item 3: flash hook/feature keys;[31]
- Punch list item 2: party hold messages;[32] and

---

28 *See, e.g.,* AirTouch at 14; BellSouth at 9; PrimeCo at 10; SBC at 9 n.14; USTA at 5.

29 *See* DOJ/FBI Proposed Rule 64.1702.

30 47 U.S.C. § 1001(2)(emphasis added).

31 *See, e.g.,* AirTouch at 16; AT&T at 8; BellSouth at 10-11; CTIA at 12-14; SBC at 10-11; TIA at 47-53; USTA at 5; U S WEST at 18-19.

32 *See, e.g.,* AirTouch at 16; AT&T at 10-11; BellSouth at 9; CTIA at 14-15; SBC at 9-10; TIA at 53-55.

- Punch list item 4: busy, ringing, and other network-generated signals.[33]

E. Carriers Are Not Required to Provide Call-Identifying Information Which Is Not "Reasonably Available" to Them

Some of the information DOJ/FBI seek does constitute call-identifying information. However, CALEA does not require carriers to provide *all* call-identifying information to law enforcement; it requires them to provide *only* that call-identifying information which "*is reasonably available to the carrier.*"[34] Congress made very clear that if call-identifying information "is not reasonably available, the carrier does not have to modify its system to make it available."[35]

The DOJ/FBI position does not take account of this "reasonably available" limitation, as illustrated by its position regarding so-called "post-cut-through" digits. Law enforcement has always received these digits and, under the industry standard, will continue to receive these digits. Law enforcement can intercept post-cut-through digits with call content order served on the local carrier serving the interception subject or with a call-identifying information order served on the long distance carrier.[36]

---

33 *See, e.g.,* AirTouch at 16; AT&T at 11-12; BellSouth at 11-12; CTIA at 15-16; SBC at 11-12; TIA at 55-61; U S WEST at 20-21.

34 47 U.S.C. § 1002(a)(2)(emphasis added).

35 House Report at 22. Thus, it is the DOJ/FBI position, not CTIA's, which has no basis in the statute. *See* DOJ/FBI at 10 ¶ 16.

36 AirTouch and others have already explained that (a) from the practical perspective of a local carrier, post-cut-through digits constitute call content and not call-identifying information, and (b) from a legal perspective, some post-cut-through digits constitute call-identifying information while other post-cut-through digits were excluded from the call-identifying information definition. *See, e.g.,* AirTouch at 16-18.

Nevertheless, DOJ/FBI want the Commission to require local carriers to provide post-cut-through digits in response to a call-identifying interception order and over a call data delivery channel.[37] DOJ/FBI make this request even though they acknowledge that CMRS providers do not now have the capability of providing post-cut-through digits, much less the capability to distinguish between those post-cut-through digits which are call-identifying information and those digits which are not.[38] DOJ/FBI simply assert: we "endorse the development of such capability" because, regardless of the development costs, such information has "important investigatory and evidentiary value to law enforcement."[39]

AirTouch does not dispute that those post-cut-through digits constituting call-identifying information can be useful to law enforcement. But the fact is that law enforcement can receive this information *today* — either with a Title III order or with a call-identifying order served on the long distance carrier.[40] Thus, as AT&T correctly observes,

> Law enforcement's real complaint is that they have to go to the trouble of getting the information from long distance carriers. However, Congress stated unequivocally that CALEA "is not intended to guarantee 'one-stop shopping' for law enforcement."[41]

---

37 *See* DOJ/FBI Petition at 38-42 ¶ 66-72 and 47-49 ¶ 83-85. DOJ/FBI may be abandoning their latter request. *See* DOJ/FBI at 12 ¶ 20. *See also* TIA at 42 ("FBI agreed that carriers can make post-cut-through digits available to law enforcement by 'provid[ing] CCC [the call content channel] to law enforcement for deciphering.'")(internal citation omitted).

38 DOJ/FBI at 11 ¶ 19 and n.2.

39 *Id.* at 10-11 ¶ 17 and n.2.

40 *See, e.g.,* AT&T at 9 n.29; PrimeCo at 13; TIA at 42-43.

41 AT&T at 10, *quoting* House Report at 22.

More fundamentally, it is undisputed that industry cannot provide post-cut-through" digits without additional development work by vendors and major system modifications by carriers.[42] As TIA observes:

> [The provision of post-cut-through digits by local carriers] would require major system modifications to dedicate a tone receiver for the duration of each call, which would be necessary to detect post-cut-through digits and deliver them to law enforcement. Costly switch modifications without any business justification would be needed to provide such capability.[43]

Consequently, it cannot be said that the provision of post-cut-through digits is "reasonably available" to the CMRS industry and, under the clear commands of CALEA, CMRS providers are under no obligation to provide these digits to law enforcement in the particular manner they demand. Law enforcement may continue to receive these digits either from interexchange carriers directly or from CMRS providers *via* a Title III order.

F. The New York City Police Department Position

The DOJ/FBI Petition is supported only by a "technical advisor" to the New York City Police Department ("NYPD"). According to this advisor, the industry standard is "plainly deficient," although he presents no legal analysis in support of this legal conclusion.[44]

Instead, the advisor claims the industry standard is deficient because, "[w]ithout the 'punch list' capabilities, law enforcement's ability to conduct effective electronic surveillance

---

42 As discussed above, DOJ/FBI have not shared with carriers — and the Commission — the estimated cost that would be incurred in developing this capability.

43 TIA at 44-45. *See also* Ameritech at 7 ("[E]xtraction of post-cut-through digits is an expensive and timely obligation to be placed on telecommunications carriers.").

44 NYPD at 1.

and the public safety will be severely compromised."[45] This unsupported allegation is simply not credible. By their punch list, law enforcement seeks capabilities and solutions *never* before provided by carriers. By definition, then, the Commission's rejection of these new punch list demands cannot possibly "compromise" the ability to conduct interceptions in the future.

There is, moreover, no evidence that New York law enforcement agencies have been hampered in their ability to conduct interceptions. During 1997, New York officials installed a total of 289 Title III "taps" — 26% of the total "taps" conducted by all law enforcement and 54% of the total "taps" conducted by state and local law enforcement.[46] New York officials also conducted a large number of electronic interceptions (*e.g.*, cellular, paging). During 1997, New York officials conducted 89 electronic "taps" — 43% of the total electronic "taps" conducted by all law enforcement and 68% of the total electronic "taps" conducted by state and local law enforcement.[47] If anything, the NYPD comments help confirm that the punch list items are not required by law enforcement to continue to conduct lawful surveillance.

II. The CDT Petition Issues: CMRS Location and Packet Switching

The Center for Democracy and Technology ("CDT") has petitioned the Commission to rule that two capabilities in the existing industry standard — limited CMRS location information and packet switched data — are inconsistent with CALEA.[48] As discussed below,

---

45 *Id.*

46 *See* Report of the Director of the Administrative Office of the U.S. Courts, *Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications*, Table 6 (April 1998).

47 *Id.*

48 CDT, Petition for Rulemaking Under Sections 107 and 109 of the Communications Assistance for Law Enforcement Act (March 26, 1998)("CDT Petition").

the controversy over CMRS location information appears to have been mooted by a change in the FBI's position. While the issues pertaining to packet switching remain difficult, AirTouch submits that, given the peculiarity of the issues involved, the matter is best addressed on a case-by-case basis by courts experienced with the scope of the nation's interception laws. As demonstrated below, the industry standard would simply enable industry to comply with any order a court may render. There is, in sum, no need for the Commission to do more in this area.

A. The CMRS Location Controversy Appears To Have Become a Non-Issue

The industry standard would permit law enforcement to receive *limited* information about the location of a CMRS subscriber *subject to a court order*. Specifically, the standard would enable law enforcement to learn the identity of the cell site serving an intercept subject at the beginning and end of a CMRS call — *not* during the call and *not* during times when the intercept subject is not using his or her handset.[49] In addition, the standard makes clear that this limited location information will be provided only when the capability "is reasonably available" to the carrier *and* the "delivery [of such information] is authorized."[50]

CDT acknowledges that law enforcement may receive this location information pursuant to a Title III order, but persuasively argues that the Congress expressly prohibited carriers from furnishing this data pursuant to the more lenient standard required to conduct a pen

---

49 *See* J-STD-025 § 6.4.6. As the FBI notes, each cell site, or base station, can serve vast areas and, under the standard, law enforcement still would not be able to identify the specific physical location of an intercept subject. *See* FBI at 19 ¶ 38 and 20 n.4.

50 *See* J-STD-025 §§ 5.4.1, 5.4.5, 5.4.6, and 5.4.8.

register or a trap-and-trace device.[51] In its comments, the FBI has reversed its position on this issue, and now appears to agree with CDT:

> Pen register orders under 18 U.S.C. § 3123 do not authorize law enforcement to acquire such location information. . . . In contrast, law enforcement can obtain location information with an appropriate Title III order or an order issued pursuant to 18 U.S.C. § 2703(d).[52]

Thus, there appears to be consensus over the circumstances when law enforcement may, and may not, obtain authority to receive the limited location information available under the industry standard.[53]

However, there does remain an ongoing dispute over whether location information is required by CALEA. For example, DOJ/FBI contend that location information is required by CALEA because, insofar as it helps identify the "origin" of the communications, location information falls within the statute's definition of call-identifying information.[54] Privacy groups and certain members of the industry counter that location information does *not* fall within the definition of call-identifying information because it does not constitute "dialing or signaling information."[55]

---

51 *See* CDT at 33 ("Under 18 U.S.C. § 2618(4), location information, if otherwise available, can be obtained under appropriate legal authority (but not under a pen register or trap and trace).").

52 DOJ/FBI at 18-19 ¶¶ 35-36 (emphasis in original).

53 Given that DOJ/FBI have changed their positions over time, AirTouch submits that it would be prudent for the Commission to restate in its order the DOJ/FBI's current position regarding CMRS location information and the need for a Title III order.

54 *See* FBI at 18 ¶ 33.

55 *See, e.g.*, CDT at 29-30; TIA at 76. *See also* 47 U.S.C. 1002(2)("The term 'call-identifying information' means *dialing or signaling information* that identifies the origin,

(continued...)

This legal issue may have little practical significance, however. This is because, whether or not location information is required by CALEA, (a) there is consensus that law enforcement is entitled to receive this information upon receipt of a Title III court order *if* the information is reasonably available to a carrier; (b) the Commission has required carriers to deploy a similar location capability under specified circumstances as part of a carrier's E911 obligation;[56] and (c) under the industry standard deemed sufficient by DOJ/FBI as to this capability, carriers are required to provide limited location information only when the information is reasonably available to the carrier.[57] Given these facts, AirTouch submits there is no reason at this time for the Commission to set forth its views as to whether location information is, or is not, required by CALEA.[58]

---

55 (...continued)
direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.") (emphasis added).

56 Commission rules provide that "[a]s of April 1, 1998, licensees subject to this section must relay . . . the location of the cell site or base station receiving a 911 call from any mobile handset . . . to the designated Public Service Answering Point" ("PSAP"). 47 C.F.R. § 20.18(d). However, carriers must comply with this requirement "only if the administrator of the designated [PSAP] has requested the services required under these paragraphs and is capable of receiving and utilizing the data elements associated with the service, and a mechanism for recovering the costs of the service is in place."). The DOJ has determined that these location requirements do not implicate our nation's interception laws. *See Public Notice,* "Memorandum Opinion Issued by Department of Justice Concludes that Commission's Recently Adopted Wireless Enhanced 911 Rules Are Consistent with Wiretap Act," 11 FCC Rcd 17305 (1996).

57 *See* J-STD-025 § 6.4.6.

58 AirTouch finds comforting the DOJ's recent statements that it is "very concerned" about "diminishing [privacy] protections on wireless communications" and about proposals that "would subject some classes of wireless electronic communications to a lower standard than other electronic communications." Letter from Ann Harkins, Acting Assistant Attorney General, to Hon. Henry Hyde, Chairman, House Judiciary Committee, at 5 and (continued...)

B. The Industry Standard Regarding Packet Switched Data Gives Carriers the Flexibility to Meet Court Interception Orders

Packet switched technology presents an anomaly under our nation's interception laws that Congress regrettably chose not to address in CALEA. Our interception laws have two different standards to conduct interceptions: (1) a more lenient standard to conduct pen registers and trap-and-trace devices — so called "call-identifying" interceptions;[59] and (2) a more rigorous standard for "call content" interceptions.[60] What standard should be applied to proposed interceptions of packet switched communications, where call identifying and call content information are combined within the same packet?

Law enforcement may unquestionably receive all packet data communications with a Title III, call content interception order. The controversy rather surrounds what law enforcement may receive, if anything, with a "call-identifying information" interception order. Privacy organizations contend that law enforcement may not receive any call content with a call-identifying information interception order,[61] and there is legal authority for this proposition.[62] DOJ/FBI counter that, even if they receive call content with a call-identifying interception order, they still are "legally precluded from recording or decoding data other than dialing and signaling

---

58 (...continued)
6 (May 20, 1998).

59 *See* 18 U.S.C. § 3123.

60 *See id.* at § 2518.

61 *See* CDT at 34-37; EPIC/EFF/ACLU at 24-25.

62 *See, e.g., Brown* v. *Waddell,* 50 F.3d 285 (4th Cir. 1995) (holding that a Title III order is required to intercept a digital display pager because interceptions would include call content).

information" because of the restrictions imposed by 18 U.S.C. § 3121(c).[63] It is unclear how courts would decide this issue, and the outcome may well be determined by the circumstances presented in each case.

The industry standard does not require carriers to remove call content from packet data if law enforcement obtains a call-identifying interception order only.[64] As TIA notes, the standard is based upon the status of telecommunications technology: "[T]echnology does not now exist to permit telecommunications carriers to provide separated packet headers as call-identifying information."[65]

CDT contends that industry's inability to separate packet content from packet call-identifying information is an "untested assumption."[66] However, some vendors have advised AirTouch that developing this separation function — so law enforcement receives only call-identifying information upon receiving only a call-identifying interception order — would be a

---

63 DOJ/FBI at 22 ¶ 41. In support, DOJ/FBI note that they are technically capable of intercepting call content with a pen register order but do not do so because of the restrictions imposed in 18 U.S.C. § 3121(c). *See id.* at 22 ¶ 43. *See also* SBC at 15.

64 *See* J-STD-025 at § 4.5.2.

65 TIA at 79. Unlike information service providers ("ISPs"), telecommunications carriers have designed their networks to transmit telecommunications — that is, "information of the user's choosing, *without change in the form or content* of the information as sent and received." 47 U.S.C. § 153(43) (emphasis added). Thus, as TIA notes, unlike ISPs, "[t]elecommunications carriers almost always carry only assembled packets, and have no reason to develop the technology (from both software and hardware) that would be required to separate packet headers from packet contents." TIA at 78-79. Clearly, providing only the call-identifying information portion of packet communications is not "reasonably available" to carriers. *See* 47 U.S.C. § 1002(a)(2).

66 *See* CDT at 34. But as BellSouth notes, it is not at all "clear the addresses contained inside packets are covered under the pen register statute." BellSouth at 17.

complex undertaking that could be expensive to provide to carriers.[67] In this regard, Congress made clear that the Commission may impose a new capability on industry only if the capability can be deployed "by cost-effective methods."[68]

The industry standard not only reflects the state of technology, but also allows courts to decide the appropriate course in the circumstances in an application for an interception order. If courts agree with privacy organizations, law enforcement will not receive any data packets without a Title III order. On the other hand, if courts decide that the FBI is correct with respect to the legal restrictions imposed by 18 U.S.C. § 3121(c), law enforcement will receive all data packets within a call-identifying interception order.

If, however, the Commission is inclined to consider CDT's proposal that carriers be required to perform the separation function for packet data, then AirTouch joins TIA's request to commence a separate rulemaking to gather further information on the proposal.[69] AirTouch (and other carriers) need an opportunity to obtain more concrete information, including cost data, from its vendor-suppliers to determine the technical and economic feasibility of this separation proposal.[70]

---

67 *See also* SBC at 16 (deploying a separation technology "would be extremely difficult and costly"). AirTouch has been unable, however, to obtain from its vendors more specific facts to document this assertion — including estimated costs to develop this separation feature. *See* discussion *supra* at 3-4.

68 47 U.S.C. § 1006(b)(1).

69 *See* TIA at 80. *See also* AT&T at 12 ("Should the Commission agree with CDT [regarding packet technology], it should undertake an analysis of the cost of modifying systems to accomplish this task.").

70 Again, it bears emphasis that CALEA requires carriers to provide only that call-identifying information that "is reasonably available to the carrier." 47 U.S.C. § 1002(a)(2). In addition, the Commission may impose a requirement on carriers only if the capability in

(continued...)

III. The Opposition to Referral of Any Additional Standards Development to TR-45.2 Lacks Merit

AirTouch submits that the record compels affirmation of the industry standard and rejection of the deficiency petitions. With respect to the standards dispute generally, there now appears to be consensus among the commenters (including DOJ/FBI) that the Commission has the statutory authority— indeed, obligation — to determine what assistance capabilities are, and are not, required by CALEA.[71] Where parties disagree is over who should develop the technical details implementing the Commission's decision so vendors can begin designing compliant equipment that will also continue to work with the equipment of other vendors — *if* the Commission determines that the industry standard is deficient in any way.

Industry, which understands the complexity of the CALEA technology and which has a keen interest in maintaining interoperability, uniformly supports allowing the TIA standards subcommittee, TR-45.2, to develop any additional implementing details which may be necessary as a result of the Commission's order.[72] As CTIA correctly observes, "this Subcommittee developed the J-STD-025 and therefore is uniquely positioned to ensure that any changes required by the Commission are integrated consistently and properly":

---

70 (...continued)
question "meets the assistance capability requirements of section 103 *by cost-effective methods.*" 47 U.S.C. § 1006(b)(1)(emphasis added).

71 *See, e.g.*, DOJ/FBI at 16 ¶ 28 ("[T]o the extent that the Commission's standards identify statutorily required capabilities, those standards will indeed be binding on the industry."). DOJ/FBI's recognition of this authority is important because they earlier suggested that carriers could provide to law enforcement capabilities which the Commission determined were not encompassed within CALEA. *See, e.g.*, DOJ/FBI Comments at 16 ¶ 30 (May 8, 1998)("The carrier will not be *required* to remove these capabilities" which the Commission determines are inconsistent with CALEA.) (emphasis in original).

72 *See, e.g.*, AirTouch at 28-29; AT&T at 15-17; CTIA at 18-22; Nextel at 13; PCIA at 6-7; PrimeCo at 22; SBC at 16-17; U S WEST at 31-33.

> The Commission should not put itself in the position of attempting to resolve differing technical comments. The consensus-based standards-setting process is designed and well-suited for such a process, which underscores the desirability of remanding any change in the standard to TR45.2.[73]

Such a remand, moreover, would be consistent with past Commission practice, where it has declined to adopt "extensive technical standards" because "industry standards-setting committees are better equipped to address precise technical requirements."[74] Importantly, even if the Commission adopts rules in these technical areas, its practice has been to cross-reference industry standards in its rules.[75]

Two commenters oppose referral to TR-45.2 of any additional implementing standards work, taking the position that the Commission instead should directly decide these kinds of technical details. EPIC/EFF/ACLU claim that they cannot participate in TR-45.2 meetings to protect privacy rights because the meetings are "effectively closed to non-law enforcement and non-telecommunications industry participants."[76] EPIC/EFF/ACLU have their facts wrong. As the Commission has noted, to qualify for ANSI accreditation, a standards organization like TR-45.2 "*must* implement certain due process requirements, including *open*

---

73 CTIA at 18-19. *See also* AirTouch at 28 ("This subcommittee is equipped to ensure that any modifications which the Commission may order are consistent with all existing standards and protocols, including the new Lawfully Authorized Electronic Surveillance ("LEAS") protocol which TR-45.2 developed specifically to implement CALEA.").

74 *Enhanced 911 Emergency Calling Systems,* 9 FCC Rcd 6170, 6177 ¶ 40 (1994). *See also Petition to Amend Part 68 to Include Terminal Equipment Connected to Public Switched Digital Service*, 11 FCC Rcd 5091, 5099 ¶ 17 (1996)(referring technical details to industry standards organizations).

75 *See, e.g.,* 47 C.F.R. §§ 1.1307(b)(4)(i), 2.948(b)(8), 15.31(a)(6), 22.602(j), 22.933, 24.237(a), 73.44(e), 74.638(a)(2).

76 EPIC/EFF/ACLU at 28-29. It is noteworthy that other privacy organizations do not make these same arguments. *See* CDT and ATR/CTP/CSE.

meetings, prior notice, and the building of consensus" and that standards meetings be "*open to the participation of anyone* with an interest in that question."[77] Indeed, another privacy organization, CDT, not only participated the CALEA standards process but also notes that industry modified the proposed standard in response to its concerns.[78] Thus, EPIC/EFF/ACLU representatives *will* be able to participate in any additional TR-45.2 standards work regarding CALEA, should they choose to attend — and they always retain the right to return to the Commission even if they choose not to attend TR-45.2 meetings.[79]

DOJ/FBI also oppose referral, claiming that referral is unnecessary because their proposed rules are set forth "in sufficient detail."[80] Suffice it to say that this view is shared by *no one* — including industry which has the obligation to design and deploy equipment consistent with the Commission's orders.[81] Indeed, the industry ESS ad hoc group recently had to delay its

---

77 *International Communications Policies Governing Designation of Recognized Private Operating Agencies*, 2 FCC Rcd 7375, 7381 n.13 (1987)(emphasis added).

78 *See* CDT at 35.

79 However, AirTouch does question the degree to which privacy concerns would be relevant to TR-45.2's work. The basic legal issues, including privacy questions, will be addressed by the Commission in its rulemaking order. The task of TR-45.2 would be limited to developing technical details and specifications implementing any order the Commission may adopt.

80 FBI at 26 ¶ 52. Completely baseless is the FBI's argument that the Commission lacks the legal authority to remand the technical details to TR-45.2. *See id.* at 24-26 ¶¶ 48-50. As commenters point out, Section 551(c) of the Telecommunications Act also requires the Commission to adopt certain "rules," which it accomplished by referring to industry standards. *See Technical Requirements to Enable Blocking of Video Programming*, ET Docket No. 97-206, *Report and Order*, FCC 98-36 (March 13, 1998). The fact that DOJ/FBI believe that the current standard is incomplete does not undermine the propriety of referring additional issues to TR-45.2 as they claim. *See* FBI at 25 ¶ 50.

81 *See, e.g.*, AirTouch at 3-4; AT&T at 16 (FBI's proposed rules are "imprecise, technically inadequate, and not compatible with J-STD-025."); U S WEST at 33. *See also* CTIA/

(continued...)